e: 3510-33-P

DEPARTMENT OF COMMERCE

Bureau of Industry and Security

15 CFR Parts 740, 772, and 774

[Docket No. 220520-0118]

RIN 0694-AH56

Information Security Controls: Cybersecurity Items

AGENCY: Bureau of Industry and Security, Commerce.

ACTION: Final rule.

SUMMARY: BIS is finalizing changes to License Exception ACE and corresponding changes in the definition section of the Export Administration Regulations (EAR) in response to public comments to an October 21, 2021 interim rule. That rule established a new control on certain cybersecurity items for National Security (NS) and Anti-terrorism (AT) reasons, as well as adding a new License Exception Authorized Cybersecurity Exports (ACE) that authorizes exports of these items to most destinations except in certain circumstances. These items warrant controls because these tools could be used for surveillance, espionage, or other actions that disrupt, deny or degrade the network or devices on it. This rule also corrects Export Control Classification Number (ECCN) 5D001 in the Commerce Control List.

DATES: This rule is effective **[INSERT DATE OF PUBLICATION IN THE FEDERAL REGISTER]**.

FOR FURTHER INFORMATION CONTACT: For questions regarding the Export Control Classification Numbers (ECCNs) included in this rule or License Exception ACE, contact Aaron Amundson at 202-482-0707 or e-mail Aaron.Amundson@bis.doc.gov.

SUPPLEMENTARY INFORMATION:

Background

In 2013, the Wassenaar Arrangement (WA) decided on new controls on cybersecurity items. The controls included hardware and software controls on the command and delivery platforms for "intrusion software", the technology for the "development", "production" or "use" of the command and delivery platforms, and the technology for the "development" of "intrusion software". On May 20, 2015, BIS published a proposed rule (80 FR 28853) entitled "Wassenaar Arrangement 2013 Plenary Agreements Implementation: Intrusion and Surveillance Items," which proposed implementing these controls and sought comments on their impact.

In response to the proposed rule, BIS received almost 300 comments that raised substantial concerns about the proposed rule's scope and the effect the proposed rule would have on legitimate cybersecurity research and incident response activities. BIS also conducted extensive outreach with the security industry, financial institutions, and government agencies that manage cybersecurity.

Comments on the previously published proposed rule focused on three main issues. First, many commenters asserted that the entries were overly broad, captured more than was intended, and, as a technical matter, failed to accurately describe the items intended for control. Second, many commenters asserted that the rule as written imposed a heavy and unnecessary licensing burden on legitimate transactions that contribute to cybersecurity. Third, many commenters suggested that the proposed rule's control on technology for the "development" of "intrusion software" could cripple legitimate cybersecurity research.

Based on these comments, the United States decided against amending the proposed rule and instead returned to the WA in 2016 and 2017 to negotiate changes to the text. In December 2017, the WA published the changes that resulted from those negotiations. There were three significant changes: first, using "command and control" in the control language for both hardware and software addressed concerns from cybersecurity companies to more specifically control tools that can be used maliciously; second, adding a note to the control entry for technology for the "development" of "intrusion software" that excludes from the entry "technology" that is exchanged for "vulnerability disclosure" or "cyber incident response"; and third, adding a note to the "software" generation, command and control, or delivery entry that excludes from this entry products designed and limited to providing basic software updates and upgrades.

On October 21, 2021 (86 FR 58205), the Bureau of Industry and Security (BIS) published an interim final rule (October 21 rule) that establishes new controls on certain cybersecurity items for National Security (NS) and Anti-terrorism (AT) reasons, along with a new License Exception, Authorized Cybersecurity Exports (ACE), that authorizes exports of these items to most destinations except in specified circumstances. That rule was published with a 45-day comment period, which ended on December 12, 2021, and a 90-day delayed effective date (January 19, 2022). A total of 12 comments were received. On January 12, 2022 (87 FR 1670), BIS published a rule that further delayed the effective date of the interim final rule by 45 days (March 7, 2022). That action did not extend or reopen the comment period for BIS's previous request for comments on the interim final rule. Consistent with the comments received, this action amends the October 21 rule that became effective March 7, 2022.

Public Comments on the October 21 rule

Comments Requesting Additional Guidance

Several commenters stated that the new 5A001.j entry is complex and therefore presents compliance difficulties. One commenter asked whether 5A001.j would control cybersecurity incident detection and monitoring software. Another commenter stated that 5A001.j systems have numerous components, all of which will need to be examined under the new entry. In response, BIS is providing additional information and guidance through "Frequently Asked Questions" (FAQs) on 5A001.j to clarify these interpretation issues. BIS does not expect 5A001.j to control a large number of products, and therefore believes these issues can be addressed in the FAQs.

Several commenters recommended that BIS devote additional resources to conducting outreach to exporters about the interim final rule. One commenter recommended a decision tool for ACE like the one used for License Exception Strategic Trade Authorization (STA), as well as more FAQs. Another said BIS should put more resources towards outreach to the cybersecurity community. One commenter recommended developing additional guidelines to help exporters with the interim final rule. BIS agrees with these comments and is working on providing additional guidance along these lines.

Several commenters asked for clarification of BIS's "reason to know" standard. One commenter said that the end-use based control uses the phrase "knows or has reason to know" and asked if this was supposed to be different from the "knowledge" standard. Others recommended BIS provide guidelines on when an exporter would have "reason to know" something will be used for unauthorized surveillance. The terms "know" and "reason to know" use the same definition found in § 772.1 of the EAR as the term "knowledge," which is the one that should be used for this rule. BIS has published extensive "Know Your Customer" guidance in supplement no. 3 to part 732 of the EAR and on its website. That information also applies to transactions under license exception ACE. BIS believes the current guidance is sufficient to address the questions raised by the commenters and declines to provide additional sector-specific guidance for this area beyond what is published on the website.

Comments Requiring Regulatory Changes

Several commenters stated that the definition of 'government end user' in ACE is vague and will be difficult to apply. Two commenters stated that there is some potential overlap between 'government end users' and 'favorable treatment cybersecurity end users'. BIS agrees with this recommendation and makes changes to the definition of 'government end user' to be more specific and to clarify the meaning of this term.

One commenter stated that the licensing requirement for people acting on behalf of a 'government end user' will chill cross-border collaboration with cybersecurity researchers and bug bounty hunters because exporters will be required to check whether an individual has a government affiliation before communicating with them. The company recommends BIS either remove this requirement or modify it. BIS disagrees with this recommendation. The license requirement for people acting on behalf of a government is necessary to prevent people who are acting on behalf of a Country Group D government from obtaining 'cybersecurity items' for activities contrary to U.S. national security and foreign policy interests. Removing this requirement would risk allowing Country Group D governments access to those items. BIS agrees that this means that exporters will in some cases have to check government affiliation of people and companies they work with. However, because of the limited scope and applicability of the license requirement, BIS believes the requirement will protect U.S. national security and foreign policy interests without unduly impacting legitimate cybersecurity activities.

A couple of commenters stated that the definitions of "vulnerability disclosure" and "cyber incident response" are too narrow. One commenter said that researchers share vulnerability information unrelated to remediation of a specific vulnerability or incident. Another said the definitions should include information that is not strictly "necessary" for vulnerability disclosure or cyber incident response activities, as well as information that is needed to prevent

cyber incidents from happening. One commenter recommended expanding the exclusion to include preventative remediation and coordination activities. They recommend two possible solutions: (1) amend FAQs to clarify that the carve-out covers routine sharing of exploits for cybersecurity purposes; or (2) amend the definition of fundamental research to include transferring exploit information for research purposes. BIS believes that many of the activities commenters mentioned as being subject to a license requirement, such as tactics and techniques of malicious actors, and identifying products that contain vulnerabilities, are not subject to this control and that therefore the scope of items that would require a license in this area is significantly smaller than the commenters asserted. Therefore, BIS is not amending the rule but will clarify the scope of license requirements in this area via guidance in FAQs.

Other Significant Comments

One commenter suggested extending the comment period to January 5, 2022. Another recommended delaying the effective date of the rule and conducting more extensive industry consultations and engagements. In response, BIS delayed the implementation date of the October 21 rule to March 7, 2022, and reached out to interested industry members of BIS's Technical Advisory Committees to prepare additional guidance and make clarifications that are in this final rule.

Several commenters said the rule is complicated and will be difficult for people to understand and implement. In response, BIS has made several changes in this final rule to clarify the scope of controls. In addition, BIS delayed the implementation date of the October 21 rule to March 7, 2022, which allowed for the preparation of additional guidance to assist with compliance.

One commenter said that the estimated yearly expense of compliance of $2,520 is a gross underestimation, because the complexity of the rule will increase the cost of compliance. However, none of the commenters provided data to substantiate this claim or provided another estimate. BIS consulted with its Technical Advisory Committees to develop the estimate yearly expense identified in this rule.

Specific Revisions

Section 740.17 License Exception Encryption Commodities, Software, and Technology (ENC)

BIS is revising § 740.17 by adding a new end-use restriction (§ 740.17(f)) equivalent to the end-use restriction in § 740.22(c)(4) of License Exception ACE, so that License Exception ENC is not authorized if the exporter, reexporter, or transferor "knows" or has "reason to know" at the time of export, reexport, or transfer (in-country), including deemed exports and reexports, that the following items will be used to affect the confidentiality, integrity or availability of information or information systems, without authorization by the owner, operator or administrator of the information system (including the information and processes within such systems): "cryptanalytic items", classified in ECCN 5A004.a, 5D002.a.3.a or c.3.a, or 5E002; network penetration tools described in § 740.17(b)(2)(i)(F), and ECCN 5E002 "technology" therefor; or automated network vulnerability analysis and response tools described in § 740.17(b)(3)(iii)(A), and ECCN 5E002 "technology" therefor. This conforming change is necessary to avoid an unintended circumstance in which the § 740.22(c)(4) License Exception ACE end-use restriction could be evaded by adding cryptographic or cryptanalytic functionality to the 'cybersecurity item' and exporting, reexporting or transferring (in-country) the resulting 'encryption item' subject to the EAR under License Exception ENC.

Section 740.22 License Exception Authorized Cybersecurity Exports (ACE)

In response to public comments, BIS is revising § 740.22. BIS is revising the definition of the term 'Government end user' as defined in § 740.22(b)(4) of License Exception ACE by adding a detailed illustrative list of end users that meet this definition. Included in the list are two types of government end users that are already defined in the EAR, "more-sensitive government end users" and "less-sensitive government end user". BIS also added a note to define 'partially operated or owned by a government or governmental authority' to guide the public in understanding this phrase, which is used in three of the listed 'government end users' related to utilities; transportation hubs and services; and retail or wholesale firms engaged in the manufacture, distribution, or provision of items or services specified in the Wassenaar Arrangement Munitions List.

BIS also revised the format of the restrictions in § 740.22(c) by collapsing the levels and moving most of the text that was in notes to subordinate paragraphs within paragraph (c). Several people commented that the double negative structure of the restrictions paragraph was confusing. BIS believes the more simplified paragraph organization will alleviate the confusion.

Finally, BIS is amending § 740.22(c)(2)(i) to correct the text, which inadvertently increased the scope of the exception. As currently written, that paragraph allows (a) exports of 'digital artifacts' to anyone in a Country Group D country that is also listed in Country Group A:6; and (b) exports of any 'cybersecurity item' to police or judicial bodies to Country Group D countries that are also listed in Country Group A:6. However, BIS intended to only allow exports of 'digital artifacts' to police or judicial bodies in Country Group D countries that are also listed in Country Group A:6 for purposes of criminal or civil investigations or prosecutions. These changes correct the text to reflect the intended scope.

Part 772 – Definitions of Terms

This rule amends the terms "Less sensitive government end users" and "More sensitive government end users" to indicate that the terms apply to cybersecurity items and are now referenced in License Exception ACE (§ 740.22).

Part 774 – Commerce Control List: ECCN 5D001

This rule corrects an error made to ECCN 5D001in the October 21, 2021 interim rule. That rule inadvertently removed 5D001.e and this rule restores 5D001.e.

Export Control Reform Act of 2018

On August 13, 2018, the President signed into law the John S. McCain National Defense Authorization Act for Fiscal Year 2019, which included the Export Control Reform Act of 2018 (ECRA), 50 U.S.C. Sections 4801–4852. ECRA provides the legal basis for BIS's principal authorities and serves as the authority under which BIS issues this rule.

Executive Order Requirements

This final rule has been designated a "significant regulatory action" under Executive Order 12866.

This rule does not contain policies with federalism implications as that term is defined under Executive Order 13132.

Paperwork Reduction Act Requirements

Notwithstanding any other provision of law, no person is required to respond to, nor shall any person be subject to a penalty for failure to comply with a collection of information subject to the requirements of the Paperwork Reduction Act (PRA) of 1995 (44 U.S.C. 3501 et seq.)

unless a valid Office of Management and Budget (OMB) Control Number is displayed. While there is no collection of information associated with using License Exception ACE, this rule does involve a collection of information currently approved under Control Number 0694-0088, *Multi-Purpose Application*. The current burden hour estimate for this collection is 29.6 minutes for a manual or electronic submission.

For the existing ECCNs included in this rule (4D001, 4E001, 5A001, 5A004, 5D001, 5E001), the 2020 data from the Automated Export System (AES) shows 980 shipments valued at $39,146,164. Of those shipments, 120 shipments valued at $1,864,699 went to Country Group D:1 or D:5 countries, which would make them ineligible for License Exception ACE. There were no shipments to Country Group E:1 or E:2. Under the provisions of this rule, the 120 shipments require a license application submission to BIS.

As there is no specific ECCN data in AES for the new export controls in new ECCNs 4A005 and 4D004 or new paragraph 4E001.c, BIS has used other data to estimate the number of shipments of these new ECCNs that will require a license. Bureau of Economic Analysis (BEA) data from 2019 show a total dollar value of $55,657,000 for Telecom, Computer, and Information Technology Services exports. Multiplying this value by 12.1% (the percentage of all exports that are subject to an EAR license requirement as determined by using AES data) suggests that $6,734,497,000 of Telecom/Computer/IT exports are now subject to EAR license requirements. Based on AES data on the existing ECCNs affected by this rule, BIS estimates the average value of each shipment for the new ECCNs at about $40,000, and further estimates that 0.6% of all new ECCN shipments (1,010 shipments) are now eligible for License Exception ACE and 0.03% of all new ECCN shipments (50 shipments) require a license application submission.

Therefore, the annual total estimated cost associated with the paperwork burden imposed by this rule (that is, the projected increase of license application submissions based on the

additional shipments requiring a license) is estimated to be 170 new applications x 29.6 minutes = 5,032/60 min = 84 hours x $30 = $2,520.

BIS is in the process of updating this information collection to account for the increase in burden hours and costs posed by this rule. Comments on the methodology associated with calculating the cost or burden increases or any other aspect of this collection can be submitted via www.regulations.gov by searching for OMB Control Number 0694-0088.

Administrative Procedure Act and Regulatory Flexibility Act Requirements

Pursuant to Section 4821 of ECRA, this action is exempt from the Administrative Procedure Act (5 U.S.C. 553) requirements for notice of proposed rulemaking and opportunity for public participation. Further, no other law requires notice of proposed rulemaking or opportunity for public comment for this final rule. Because a notice of proposed rulemaking and an opportunity for public comment are not required under the Administrative Procedure Act or by any other law, the analytical requirements of the Regulatory Flexibility Act (5 U.S.C. 601 et seq.) are not applicable.

List of Subjects

15 CFR Part 740

Administrative practice and procedure, Exports, Reporting and recordkeeping requirements.

15 CFR Part 772

Exports.

15 CFR Part 774

Exports, Reporting and recordkeeping requirements.

Accordingly, the interim rule amending 15 CFR parts 740, 772, and 774, which was published on October 21, 2021 (86 FR 58205), is adopted as final with the following changes:

PART 740 [AMENDED]

1. The authority citation for part 740 continues to read as follows:

Authority: 50 U.S.C. 4801-4852; 50 U.S.C. 4601 *et seq.*; 50 U.S.C. 1701 *et seq.*; 22 U.S.C. 7201 *et seq.*; E.O. 13026, 61 FR 58767, 3 CFR, 1996 Comp., p. 228; E.O. 13222, 66 FR 44025, 3 CFR, 2001 Comp., p. 783.

2. Section 740.17 is revised by adding paragraph (f) to read as follows:

§ 740.17 Encryption commodities, software, and technology (ENC).

* * * * *

(f) *End-use restrictions*. Notwithstanding the other provisions and authorizations of this section, License Exception ENC is not authorized for any of the following items if the exporter, reexporter, or transferor "knows" or has "reason to know" at the time of export, reexport, or transfer (in-country), including deemed exports and reexports, that the item will be used to affect the confidentiality, integrity, or availability of information or information systems, without authorization by the owner, operator, or administrator of the information system (including the information and processes within such systems):

(1) "Cryptanalytic items," classified in ECCN 5A004.a, 5D002.a.3.a or c.3.a, or 5E002;

(2) Network penetration tools described in paragraph (b)(2)(i)(F) of this section, and ECCN 5E002 "technology" therefor; or

(3) Automated network vulnerability analysis and response tools described in paragraph (b)(3)(iii)(A) of this section, and ECCN 5E002 "technology" therefor.

Note to paragraph (f): See also § 740.22(c)(4).

3. Section 740.22 is revised to read as follows:

§ 740.22 Authorized Cybersecurity Exports (ACE).

(a) *Scope*. License Exception ACE authorizes export, reexport, and transfer (in-country), including deemed exports and reexports, of 'cybersecurity items,' as set forth in paragraph (b) of this section, subject to the restrictions set forth in paragraph (c) of this section. Deemed exports and reexports are authorized under this license exception, except for deemed exports or reexports to E:1 and E:2 nationals as described in paragraph (c)(1) of this section, to certain 'government end users' as described in paragraph (c)(2) of this section, and subject to the end use restrictions described in paragraph (c)(4) of this section. Even if License Exception ACE is not available for a particular transaction, other license exceptions may be available. For example, License Exception GOV (§ 740.11) authorizes certain exports to U.S. Government agencies and personnel. License Exception TMP (§ 740.9(a)(1)) authorizes the export, reexport, and transfer (in country) of tools of the trade in certain situations.

(b) *Definitions*. The following terms and definitions are for the purpose of License Exception ACE only.

(1) '*Cybersecurity Items'* are ECCNs 4A005, 4D001.a (for 4A005 or 4D004), 4D004, 4E001.a (for 4A005, 4D001.a (for 4A005 or 4D004) or 4D004), 4E001.c, 5A001.j, 5B001.a (for 5A001.j), 5D001.a (for 5A001.j), 5D001.c (for 5A001.j or 5B001.a (for 5A001.j)), and 5E001.a (for 5A001.j or 5D001.a (for 5A001.j)).

(2) *'Digital artifacts'* are items (*e.g.,* "software" or "technology") found or discovered on an information system that show past or present activity pertaining to the use or compromise of, or other effects on, that information system.

(3) *'Favorable treatment cybersecurity end user'* is any of the following:

(i) A "U.S. subsidiary";

(ii) Providers of banking and other financial services;

(iii) Insurance companies; or

(iv) Civil health and medical institutions providing medical treatment or otherwise conducting the practice of medicine, including medical research.

(4) *'Government end user,'* for the purpose of this section, is a national, regional, or local department, agency, or entity that provides any governmental function or service, including entities or individuals who are acting on behalf of such an entity. This term does not include any 'favorable treatment cybersecurity end user' listed in paragraph (b)(3) of this section. This term includes, but is not limited to:

(i) International governmental organizations;

(ii) Government operated research institutions;

(iii) "More-sensitive government end users";

(iv) "Less-sensitive government end users";

(v) Utilities (including telecommunications service providers and internet service providers) that are wholly operated or owned by a government or governmental authority or 'partially operated or owned by a government or governmental authority';

(vi) Transportation hubs and services (*e.g.,* airlines and airports; ships and ports; railways and rail stations; buses, trucking and highways) that are wholly operated or owned by a government or governmental authority or 'partially operated or owned by a government or governmental authority'; and

(vii) Retail or wholesale firms that are wholly operated or owned by a government or governmental authority or 'partially operated or owned by a government or by a governmental authority', engaged in the manufacture, distribution, or provision of items or services specified in the Wassenaar Arrangement Munitions List.

(5) For the purposes of this section, *'partially operated or owned by a government or governmental authority'* means that a foreign government or governmental authority beneficially owns or controls (whether directly or indirectly) 25 percent or more of the voting securities of the foreign entity, or a foreign government or governmental authority has the authority to appoint a majority of the members of the board of directors of the foreign entity.

(c) *Restrictions*. License Exception ACE does not authorize deemed exports and reexports, exports, reexports, or transfers (in-country) of 'cybersecurity items' as follows:

(1) To a destination that is listed in Country Group E:1 or E:2 in supplement no.1 to this part.

(2) To a 'government end user', as defined in this section, of any country listed in Country Group D:1, D:2, D:3, D:4 or D:5 in supplement no. 1 to this part, *except*:

(i) 'Digital artifacts' (that are related to a cybersecurity incident involving information systems owned or operated by a 'favorable treatment cybersecurity end user') to police or

judicial bodies in Country Group D countries that are also listed in Country Group A:6 for purposes of criminal or civil investigations or prosecutions of such cybersecurity incidents; *or*

(ii) To national computer security incident response teams in Country Group D countries that are also listed in Country Group A:6 of 'cybersecurity items' for purposes of responding to cybersecurity incidents, for purposes of "vulnerability disclosure", or for purposes of criminal or civil investigations or prosecutions of such cybersecurity incidents.

(3) The restrictions in paragraphs (c)(1) and (2) of this section also apply to activities, including exports, reexports, and transfers (in-country), related to "vulnerability disclosure" and "cyber incident response".

Note 1 to paragraph (c)(3): For paragraphs (c)(1) and (2) of this section, see Note 1 to ECCN 4E001 in the CCL (supplement no. 1 to part 774 of the EAR) excluding "vulnerability disclosure" and "cyber incident response" from control under 4E001.a or .c.

(4) To a non-'government end user' located in any country listed in Country Group D:1 or D:5 of supplement no. 1 to this part, *except*:

(i) Cybersecurity items classified under ECCNs 4A005, 4D001.a (for 4A005 or 4D004), 4D004, 4E001.a (for 4A005, 4D001.a (for 4A005 or 4D004) or 4D004) and 4E001.c, to any 'favorable treatment cybersecurity end user'.

(ii) "Vulnerability disclosure" or "cyber incident response".

(iii) Deemed exports.

(5) If the exporter, reexporter, or transferor "knows" or has "reason to know" at the time of export, reexport, or transfer (in-country), including deemed exports and reexports, that the

'cybersecurity item' will be used to affect the confidentiality, integrity, or availability of information or information systems, without authorization by the owner, operator, or administrator of the information system (including the information and processes within such systems).

PART 772 [AMENDED]

4. The authority citation for part 772 continues to read as follows:

Authority: 50 U.S.C. 4801-4852; 50 U.S.C. 4601 et seq.; 50 U.S.C. 1701 et seq.; E.O. 13222, 66 FR 44025, 3 CFR, 2001 Comp., p. 783.

5. Section 772.1 is amended by revising the definitions "Less sensitive government end users" and "More sensitive government end users" to read as follows:

§ 772.1 Definitions of terms as used in the Export Administration Regulations (EAR).

*****

Less sensitive government end users (as applied to encryption items and 'cybersecurity items'). The following "government end users" (as defined in this section) are considered "less sensitive" for the purposes of License Exception ENC (§ 740.17 of the EAR) and License Exception ACE (§ 740.22 of the EAR):

(1) Local/state/provincial "government end users" (departments, agencies, and entities), including local/state/provincial executive, legislative, judicial, police, fire, rescue, and public safety agencies.

(2) National/federal/royal "government end users" (departments, agencies, and entities) providing the following civil government functions and services:

(i) Census and statistics services;

(ii) Civil public works infrastructure services (construction, maintenance, repair, regulation, and administration) as follows: Buildings, public transportation, roads and highways, trucking;

(iii) Civil service administration and regulation, including human resources and personnel/labor management;

(iv) Clean water infrastructure services (treatment, supply and testing);

(v) Economic (trade/commerce/investment), business and industrial development, promotion, regulation and administration, excluding the following end users/end uses:

(A) Agencies, departments, boards, and councils for science and technology;

(B) Research, development, and national laboratories (other than as specified in paragraphs (2)(xi) (measurements and standards services) and (2)(xii) (meteorology/weather/atmospheric services) of this definition); and

(C) National telecommunications and information technology agencies, boards, councils, and development authorities (including national information center, and Information Communications Technology (ICT)/telecommunications infrastructure/spectrum planning, policy, regulation, and testing);

(vi) Elections, balloting, and polling services;

(vii) Energy regulation and administration, including oil, gas, and mining sectors;

(viii) Environmental/natural resources regulation, administration, and protection, including wildlife, fisheries, and national parks;

(ix) Food/agriculture regulation and administration;

(x) Labor/community/social services planning, regulation, and administration, including: housing and urban development, municipality and rural affairs;

(xi) Measurements and standards services;

(xii) Meteorology (weather, atmospheric) services;

(xiii) National archives/museums;

(xiv) Patents;

(xv) Pilgrimage and religious affairs;

(xvi) Postal services;

(xvii) Public and higher education (excluding government research institutions and any agency, institution, or affiliate engaged in the manufacture or distribution of items or services controlled on the Wassenaar Munitions List);

(xviii) Public health and medicine/pharmaceutical regulation and administration;

(xix) Public libraries;

(xx) Sports/culture (includes film, commercial broadcasting, and the arts) promotion, regulation, and administration; and

(xxi) Travel/tourism promotion, regulation, and administration.

* * * * *

More sensitive government end users (as applied to encryption items and 'cybersecurity items'). The following national/federal/royal (departments, agencies, and entities) "government

end users" (as defined in this section) providing the following government functions and services, are considered "more sensitive" for the purposes of License Exception ENC (§ 740.17 of the EAR) and License Exception ACE (§ 740.22 of the EAR):

(1) Agencies, departments, boards, and councils for science and technology (including research, development, and state/national laboratories, but not including measurements and standards);

(2) Currency and monetary authorities (including departments and offices of the national/federal/royal reserve);

(3) Executive agents of state (including offices of president/vice president/prime minister, royal courts, national security councils, cabinet/council of ministers/supreme councils/executive councils, crown princes and other deputies of the rulers, departments and offices of political/constitutional/mainland affairs);

(4) Legislative bodies responsible for the enactment of laws;

(5) Import/export control, customs and immigration agencies, and entities;

(6) Intelligence agencies and entities;

(7) Judiciary (including supreme courts and other national/federal/regional/royal high courts and tribunals);

(8) Maritime, port, railway, and airport authorities;

(9) Military and armed services (including national guard, coast guard, security bureaus, and paramilitary);

(10) Ministries, departments, and garrisons of defense (including defense technology agencies);

(11) Ministries and departments of finance and taxation (including national/federal/royal budget and revenue authorities);

(12) Ministries and departments of foreign affairs/foreign relations/consulates/embassies;

(13) Ministries of interior, internal/home/mainland affairs, and homeland security;

(14) State/national telecommunications and information technology agencies, boards, councils, and development authorities (including national information/critical infrastructure data centers, and Information and Communications Technology (ICT)/telecommunications infrastructure/spectrum planning, policy, regulation, and testing);

(15) Police, investigation and other law enforcement agencies, and entities (including digital crime/cybercrime/computer forensics, counter narcotics/counter terrorism/counter proliferation agencies);

(16) Prisons; and

(17) Public safety agencies and entities (including national/federal/royal agencies and departments of civil defense, emergency management, and first responders).

*****

PART 774 [AMENDED]

6. The authority citation for part 774 continues to read as follows:

Authority: 50 U.S.C. 4801-4852; 50 U.S.C. 4601 et seq.; 50 U.S.C. 1701 et seq.; 10 U.S.C. 8720; 10 U.S.C. 8730(e); 22 U.S.C. 287c, 22 U.S.C. 3201 et seq.; 22 U.S.C. 6004; 42

U.S.C. 2139a; 15 U.S.C. 1824; 50 U.S.C. 4305; 22 U.S.C. 7201 et seq.; 22 U.S.C. 7210; E.O. 13026, 61 FR 58767, 3 CFR, 1996 Comp., p. 228; E.O. 13222, 66 FR 44025, 3 CFR, 2001 Comp., p. 783.

7. In supplement no. 1 to part 774, Category 5 – Part 1, ECCN 5D001 is revised to read as follows:

Supplement No. 1 to Part 774 – The Commerce Control List

* * * * *

5D001 "Software" as follows (see List of Items Controlled).

License Requirements

Reason for Control: NS, SL, AT

Control(s)	*Country Chart (See Supp. No.1 to part 738)*
NS applies to entire entry	NS Column 1
SL applies to the entire entry as applicable for equipment, functions, features, or characteristics controlled by 5A001.f.1	A license is required for all destinations, as specified in § 742.13 of the EAR. Accordingly, a column specific to this control does not appear on the Commerce Country Chart (Supplement No. 1 to Part 738 of the EAR). ***Note to SL paragraph**: This licensing requirement does not supersede, nor does it implement, construe or limit the scope of any criminal statute, including, but not*

	limited to the Omnibus Safe Streets Act of 1968, as amended.
AT applies to entire entry	AT Column 1.

Reporting Requirements

See § 743.1 of the EAR for reporting requirements for exports under License Exceptions, and Validated End-User authorizations.

List Based License Exceptions (See Part 740 for a description of all license exceptions)

TSR: Yes, except for exports and reexports to destinations outside of those countries listed in Country Group A:5 (See Supplement No. 1 to part 740 of the EAR) of "software" controlled by 5D001.a and "specially designed" for items controlled by 5A001.b.5 and 5A001.h, and N/A for "software" classified under ECCN 5D001.a (for 5A001.j) or 5D001.c (for 5A001.j or 5B001.a (for 5A001.j)).

ACE: Yes for 5D001.a (for 5A001.j) and 5D001.c (for 5A001.j or 5B001.a (for 5A001.j)), except to Country Group E:1 or E:2. See §740.22 of the EAR for eligibility criteria.

Special Conditions for STA

STA: License Exception STA may not be used to ship or transmit 5D001.a "software" "specially designed" for the "development" or "production" of equipment, functions or features, specified by ECCN 5D001.a (for 5A001.j) and 5D001.c (for 5A001.j or 5B001.a (for 5A001.j)) to any of the destinations listed in Country

Group A:5 or A:6 (See Supplement No.1 to part 740 of the EAR); 5A001.b.3, .b.5 or .h; and for 5D001.b. for "software" "specially designed" or modified to support "technology" specified by the STA paragraph in the License Exception section of ECCN 5E001 to any of the destinations listed in Country Group A:6.

List of Items Controlled

Related Controls: See also 5D980 and 5D991.

Related Definitions: N/A

Items:

a. "Software" "specially designed" or modified for the "development", "production" or "use" of equipment, functions or features controlled by 5A001;

b. [Reserved]

c. Specific "software" "specially designed" or modified to provide characteristics, functions or features of equipment, controlled by 5A001 or 5B001;

d. "Software" "specially designed" or modified for the "development" of any of the following telecommunication transmission or switching equipment:

d.1.[Reserved]

d.2. Equipment employing a "laser" and having any of the following:

d.2.a. A transmission wavelength exceeding 1,750 nm; *or*

d.2.b. Employing analog techniques and having a bandwidth exceeding 2.5 GHz; *or*

***Note**: 5D001.d.2.b does not control "software" "specially designed" or modified for the "development" of commercial TV systems.*

d.3. [Reserved]

d.4. Radio equipment employing Quadrature-Amplitude-Modulation (QAM) techniques above level 1,024.

e. "Software", other than that specified by 5D001.a or 5D001.c, "specially designed" or modified for monitoring or analysis by law enforcement, providing all of the following:

e.1. Execution of searches on the basis of "hard selectors" of either the content of communication or metadata acquired from a communications service provider using a 'handover interface'; *and*

Technical Notes:

1. *For the purposes of 5D001.e, a 'handover interface' is a physical and logical interface, designed for use by an authorised law enforcement authority, across which targeted interception measures are requested from a communications service provider and the*

results of interception are delivered from a communications service provider to the requesting authority. The 'handover interface' is implemented within systems or equipment (e.g., mediation devices) that receive and validate the interception request, and deliver to the requesting authority only the results of interception that fulfil the validated request.

2. *'Handover interfaces' may be specified by international standards (including but not limited to ETSI TS 101 331, ETSI TS 101 671, 3GPP TS 33.108) or national equivalents.*

e.2. Mapping of the relational network or tracking the movement of targeted individuals based on the results of searches on content of communication or metadata or searches as described in 5D001.e.1.

***Note**: 5D001.e does not apply to "software" "specially designed" or modified for any of the following:*

a. Billing purposes;

b. Network Quality of Service (QoS);

c. Quality of Experience (QoE);

d. Mediation devices; or

e. Mobile payment or banking use.

*****

Matthew S. Borman,

Deputy Assistant Secretary for Export Administration.

[FR Doc. 2022-11282 Filed: 5/25/2022 8:45 am; Publication Date: 5/26/2022]